Scadenza e registrazione automatica dei certificati per la nuova registrazione automatica nella CA Cisco IOS

Sommario

Introduzione

Tutti i certificati digitali hanno un tempo di scadenza predefinito nel certificato assegnato dal server CA che rilascia il certificato durante la registrazione. Quando si utilizza un certificato digitale per l'autenticazione IPSec VPN di ISAKMP, viene eseguito un controllo automatico della scadenza del certificato del dispositivo in comunicazione e dell'ora di sistema del dispositivo (endpoint VPN). In questo modo si garantisce che un certificato utilizzato sia valido e non sia scaduto. Inoltre, è *necessario* impostare l'orologio interno su ciascun endpoint VPN (router). Se il protocollo NTP (Network Time Protocol) (o SNTP (Simple Network Time Protocol) non è disponibile sui router VPN crypto, usare il comando **set clock** manuale.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni di questo documento si basano su tutti i router che eseguono l'immagine cXXXX-advsecurityk9-mz.123-5.9.T per la rispettiva piattaforma.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Quando un certificato digitale è considerato scaduto o non scaduto?

- Un certificato è scaduto (non valido) se l'ora di sistema è successiva all'ora di scadenza del certificato o precedente all'ora di rilascio del certificato.
- Un certificato non è scaduto (valido) se l'ora di sistema è uguale o compresa tra l'ora di rilascio del certificato e l'ora di scadenza del certificato.

La funzione di registrazione automatica ha lo scopo di fornire all'amministratore della CA un meccanismo che consenta a un router attualmente registrato di eseguire automaticamente una nuova registrazione con il proprio server CA su una percentuale configurata della durata del certificato del router. Si tratta di una caratteristica importante per la gestibilità/supportabilità dei certificati come meccanismo di controllo. Se si utilizza una determinata CA per rilasciare certificati a migliaia di router VPN di filiali con una durata di un anno (senza registrazione automatica), in un anno esatto dal rilascio tutti i certificati scadranno e tutte le filiali perderanno la connettività tramite IPSec. In alternativa, se la funzione di registrazione automatica è impostata su "auto-enroll 70", come nell'esempio, nel 70% della durata del certificato rilasciato (1 anno), ogni router invia automaticamente una nuova richiesta di registrazione al server CA Cisco IOS® elencato nel trust point.

Nota: un'eccezione alla funzione di registrazione automatica è che se è impostata su un valore *minore o uguale a 10*, il valore è espresso in minuti. Se è *maggiore di 10*, rappresenta una percentuale della durata del certificato.

Esistono alcune avvertenze di cui l'amministratore della CA di Cisco IOS deve essere a conoscenza con la registrazione automatica. Affinché la nuova registrazione abbia esito positivo, l'amministratore deve eseguire le azioni seguenti:

1. Concedere o rifiutare manualmente ogni richiesta di nuova registrazione sul server CA Cisco IOS (a meno che sul server CA Cisco IOS non venga utilizzata l'opzione "grant auto").Il server CA Cisco IOS deve ancora concedere o rifiutare ciascuna di queste richieste (con il presupposto che per la CA Cisco IOS non sia abilitata la funzione di "concessione automatica"). Tuttavia, per avviare il processo di nuova registrazione, non è necessaria alcuna azione amministrativa sul router di registrazione.
2. Salvare il nuovo certificato registrato nuovamente nel router VPN di nuova registrazione, se appropriato.Se nel router non sono presenti modifiche della configurazione non salvate in sospeso, il nuovo certificato viene automaticamente salvato nella NVRAM (Non-Volatile RAM). Il nuovo certificato viene scritto nella NVRAM e il certificato precedente viene rimosso.Se sono presenti modifiche alla configurazione non salvate in sospeso, è necessario usare il comando **copy run start** sul router di registrazione per salvare le modifiche alla configurazione e il nuovo certificato registrato nella NVRAM. Una volta completato il comando **copy run start**, il nuovo certificato viene scritto nella NVRAM e il certificato precedente viene rimosso.**Nota:** se la nuova registrazione ha esito positivo, *non viene* revocato il certificato precedente per il dispositivo registrato sul server CA. Quando i dispositivi VPN comunicano, si inviano reciprocamente il numero di serie del certificato (un numero univoco).**Nota:** ad esempio, se si è al 70% della durata del certificato e un ramo VPN deve eseguire nuovamente la registrazione con la CA, tale CA dispone di due certificati per

quel nome host. Tuttavia, il router che effettua la registrazione ne ha solo uno (quello più recente). Se lo si desidera, è possibile revocare il vecchio certificato in modo amministrativo o impostarne la normale scadenza.**Nota:** le versioni più recenti del codice della funzione di registrazione automatica dispongono di un'opzione per "rigenerare" le coppie di chiavi utilizzate per l'iscrizione.Questa opzione non è di default per la rigenerazione delle coppie di chiavi.Se è stata scelta questa opzione, tenere presente l'ID bug Cisco CSCea90136. Questa correzione rapida consente di inserire la nuova coppia di chiavi in file temporanei mentre la registrazione del nuovo certificato viene eseguita su un tunnel IPSec esistente (che utilizza la vecchia coppia di chiavi).La registrazione automatica consente di generare nuove chiavi al momento del rinnovo della certificazione. Al momento ciò provoca una perdita di servizio durante il tempo necessario per ottenere un nuovo certificato. Ciò è dovuto alla presenza di una nuova chiave ma di nessun certificato corrispondente.Questa funzionalità conserva la chiave e il certificato precedenti fino a quando non sarà disponibile il nuovo certificato.La generazione automatica di chiavi è implementata anche per la registrazione manuale. Le chiavi vengono generate (se necessario) per l'iscrizione automatica o manuale.Versione trovata - 12.3PIH03Versione da correggere in - 12.3TVersione applicata a - 12.3PI03Integrato in - NessunoPer ulteriori informazioni, contattare il supporto tecnico Cisco.

Informazioni correlate

- Pagina di supporto per IPSec
- Supporto tecnico – Cisco Systems